Secure Multicasting Survey

Ghassan Chaddoud, Isabelle Chrisment, André Schaff

Secure Multicasting Survey

Ghassan Chaddoud Isabelle Chrisment André Schaff
LORIA - INRIA
Campus Scientifique - BP239
54506 Vandœuvre-Les-Nancy - FRANCE
{ chaddoud,ichris,schaff}@loria.fr

Abstract

With emerging of new cooperative applications, the group communication is clearly become a very important concept within the network architecture. The multicast transmission is appeared as the most efficient way to send some data to a specific group composed of several members. Moreover, the increasing interest in network communication through the using of the Internet requires somes services such as authentication, integrity and confidentiality to transport securely data. In this paper we present a survey about secure multicasting. We describe the different approaches existing to distribute and manage the keys within a group. We point out how the IP multicast security deals with. We show that presently no security model meets fully the requirements needed for group communication.

1. Introduction

The rapid evolution technology towards high-speed networks and processors have led to specific communication needs to meet the requirements of applications such as audio and video conferencing, shared whiteboard... By the way, the group communication is clearly become a very important concept within the network architecture. The multicast transmission appears as the most efficient way to send some data to multiple receivers by reducing the use of a lot of network bandwidth.

Moreover, the increasing interest in network communication through the using of the Internet requires some services such as authentication, integrity and confidentiality to transport securely data.

A lot of research have been achieved to protect the unicast communication and some standards are emerging ([1, 13, 15],...). But group communication makes more complex the well-known security models. It involves some specific issues which can have an influence on the security architecture [7]: group size and scalability, multicast application type(one-to-many or many-to-many), duration of group life, heterogenity of group members,... .

The purpose of this paper is to present a survey about network security within group communication and the current related research works. The paper will be organized as follows. We shall first present the secure multicasting issues, more especially the scalability issues. In order to provide security services, the entities must shared some security parameters. Section 3 will describe the management of these security parameters. Section 4 will explain the different proposed approaches for the building and the distribution of the group key, the main component of the group security parameters. Section 5 will point out the main research works achieved within the Internet world and presented at the IETF. Finally, we conclude in Section 6.

2. Secure Multicasting Issues

Like all multicast protocols, multicast security protocol exhibit two types of scalability failures summarized by MITTRA [16]: **1 affect n** which occurs when a group member affects all the other members and **1 does not equal n** which occurs when a protocol has to deal with each member separately.

The joining of a new member exhibits only the first failure type and the leaving of a member presents both types. In order to ensure forward secrecy, when a new member joins the group, the entity responsible for key management, the key manager, must replace the group key (the shared key among group members and used to encipher the group communication) by another one. The key manager multicasts the new group key to all group members using one message encrypted with the old group key. Consequently, the joining of only one member forces all the other members to change the group key ; **1** member affects the **n**(group size) other members.

To ensure backward secrecy, when a member leaves the group, the key manager must replace the group key. To do this, it needs n unicast messages to distribute the new key to every member apart through secure unicast tunnels. So, in this case, both types of scalability failure are exhibited. The first one is **1 does not equal n** when the key manager sends the new key to each member as this last one

were independent of the group. The second one is **1 affect n** because the leaving of only one member involves the modification of the key for the whole group.

Other scalability issues are induced by the lack of synchronization between the group members during group key update.

- Receivers who cannot obtain the new key become unable to decrypt the group traffic. Moreover, they can receive multicast communications from old members.
- Senders who cannot obtain the new key continue to encrypt their messages with the old key. The messages will be understood only by the members having leaved the group.

The synchronization problems can be solved by using reliable multicast protocols.

Thus far, we have described the issues of the secure multicasting, in the following section we will talk about the group security management.

3 Group security management

A security protocol must allow authorized entities to communicate securely over an insecure network where intruder can read, eliminate or modify network data. This is achieved by creating a security association[1], SA(encryption algorithms and keys, authentication algorithms and keys, SA life duration, ...) between the authorized entities through authentication and key exchange protocols. In unicast (multicast) communication, the set of these parameters is called the unicast (group) security association, SA (GSA) [1, 12].

Contrary to the SA which is managed by the two communicating entities, the security association of a group cannot be controlled by all the participants. The management of the security association of a group means the management of the group security, in particularly access control to the group (i.e. to multicast traffic of the group).

In the literature, we distinguish between two strategies for multicast security management : centralized management and decentralized management.

- the centralized management is defined by the fact that only one entity controls the group security [14, 19, 20]. And, all group members share the same key used to encrypte multicast group traffic.
- the second strategy consists of decentralizing the group management [16, 11, 12] and dividing the multicast group into sub-groups. Each sub-group, managed by a local controller, has its own key. The sub-groups are linked by intermediate agents for constructing virtual group.

The comparison between these two strategies shows that the second one presents a solution to the scalability failure **1 affect n**. Members joining or leaving affect only the sub-group to which the member belongs. Consequently, this strategy fits better the dynamic groups. But, it is less effective for diffusion of group data which undergoes encryption/decryption operations by the intermediate agents. On the other hand, the first strategy is more efficient for data diffusion because it uses only one key shared between group members. The problem of this strategy is the centralization of the group management : only one entity controls the group. When this entity breaks down, the group becomes out of control, even out of operation.

4 Group key distribution

In order to ensure confidentiality to group communications, the group members share a secret called group key (or multicast key), k_grp. A multicast message sent by a group member and encrypted with k_grp can be received and decrypted by all the members who have the same key (i.e. k_grp). The entity responsible for this key is the manager or the controller of the group, GC. This entity creates and distributes the key, in a secure manner, to the different members of the group.

4.1 The different approaches

The approaches used for the construction and the distribution of the group key fall, according to [2], into five categories : approaches based on the information theory, hybrid approaches, Diffie-Hellman key exchange approaches, SKDC (Single Key Distribution Center) and hierarchical approaches.

The information-theoric approaches are based on the information theory. BLUNDO AND ALL [4] propose a scheme for distributing key for dynamic conferences. A trusted server distributes private and individual pieces of information to a set of users. Later, a determined size subset of these users can calculate a secure shared key. Each user calculates the shared key from the identities of other users and his own piece of information.

The hyprid approaches scale linearly, or worth, in group size. They reduce the storage space by finding a compromise between different security strategies of information-theoric. This is the case of [10] which allows a central site to diffuse secure transmission to an arbitrary set of users. Let us consider a center and a group of users. The center provides each member in the group with a set of keys. At a given time, the center transmits a message to a privileged subset of users so that the other users cannot decrypt this message. Each participant in the privileged subset must be able to calculate the key to be used for deciphering the message.

In the case of the approaches of Diffie-Hellman for groups [18, 5], each group member *i* contributes to the construction of the group key by a nonce N_i. The group key is q^S mod p ; where S is the product of N_i ($i \in \{1...n\}$).These approaches offer a distributed functionality of calculation, but they suffer from a significant linear number of costly public key operations.

The approaches SKDC [14, 19] use a technique of public-key exchange (e.g Diffie-Hellman key) for creating and distributing the group key to the other participants. The number of exchanged messages due to eviction or addition of a member, and the computational operations carried out by the group manager is of the order of n (n is the group size).

Finally, we find in the last category the hierarchical approaches which scale logarithmically in group size. We can distinguish between two types : the approaches requiring trusted routers such as SMKD (Scalable Multicast Key Distribution) [3] and the approaches which do not require trusted intermediate nodes. This is the case, for example, of LKH (Logical Key Hierarchy) [19, 20] and OFT (One-way function Tree) [2].

SMKD requires trusted routers and is based on CBT (Core Based Tree) multicast protocol. The disadvantage of this approach is that it depends on routing protocols (here CBT multicast protocol); this comes up scalability problems when it is used with other routing protocols. In other words, SMKD is limited by intra-domain where the CBT multicast protocol exists. LKH and OFT propose a compromise between temporal cost, storage space and exchanged message number [19, 20]. In order to facilitate the distribution of the group key, they use a hierarchy of auxiliary keys (intermediate logic nodes). The result is that the storage space required for each member and the number of transmissions needed to re-key the group are logarithmic with the group size.

4.2 Comparative Analysis

Unfortunately, in order to ensure a long-term security against coalition of evicted members, the information-theory approaches need an exponential storage space. Also, Diffie-Hellman solutions for groups are very expensive. Generally, for the approaches based on information-theory, public key cryptography (e.g D-H for groups), hyprid and SKDC, the storage space, computation and exchanged message number increase linearly with the group size (participant number) for addition and eviction of a member. While these requirements increase logarithmically for the hierachical approaches.

In addition, the first three categories are theoretic [2] and the security for some approaches of them is not yet proven. As for SKDC and hierarchical approaches, they are more practical. The rest of this subsection will be dedicated to analyze and to compare SKDC and the both hierarchical methods LKH and OFT.

We can consider SKDC as the simplest approach. However, since it does not solve the two scalability failures : **1 affect n** and **1 does not equal n**, SKDC fits essentially small groups of discussion.

The result of comparison [2] of computational and transmission requirements at the initialization of a group shows that the size of broadcast messages for LKH and OFT is the double of that for SKDC. This results from the fact that each key of a binary tree of n leaves must be diffused to all group members. Consequently, the initialization of SKDC is faster and less costly than the two other methods.

Also, the comparaison of the manager transmission requirements for SKDC, LKH, and OFT in the case of addition or eviction of a member [2] shows that, in the case of SKDC, the manager transmission requirements is nk (where n is the group size and k is the size of cryptographic key), while this one is $2hk+h$ (h is the tree height) for LKH and $hk + h$ for OFT. Therefore, OFT carries out less transmission. Generally, LKH and OFT are more efficient than SKDC.

The comparaison of storage requirements [2] for the three approaches shows that SKDC requires a storage space less significant than LKH and OFT.

In summary, during group initialization, the approach SKDC is more efficient than the hierarchical approaches. Moreover, it requires a storage space less significant than others. On the other hand, the hierarchical approaches are more effective for dynamic groups ; because they distribute the computational cost of re-keying among the whole group. Finally, we note that OFT and LKH solve the scalability failure **1 does not equal n** by means of hierarchy of keys.

In the following section, we will present works done by the IETF to standardize IP multicast security based on unicast security standards.

5 IP multicast security

Recently, many works [6, 7, 11, 14, 3] done by IETF, have dealt with the multicast security on Internet. Among these works CANETTI AND ALL [6] suggested an architecture of IP multicast security. This architecture tries to reuse IPsec mechanisms as far as possible.

It separates the control plan of the data plan. The first one contains modules responsible for the membership management and the group access control. The second one contains modules responsible for multicast data distribution and the operations of authentication and encryption. The module MIKE (Multicast Internet Key Exchange), inspired by IKE[13], is responsible for the management of keys and the multicast security association.

Most of the other propositions are concentrated on multicast key management and can be incorporated into the module MIKE. Also [11, 12] suggest that the multicast group has to be divided into sub-groups distributed on regions. Each region is defined from the protocols and the entities available in the network infrastructure. The main disadvantage of this solution is that it imposes supplementary processing on multicast data exchanged between regions and consequently a reduction of the bandwidth on the network. Moreover, it is based on protocols of unicast

key distribution to distribute keys for group members.

BALLARDIE [3] also, proposes a solution to the scalability problem of the multicast key distribution. This solution is based on CBT (Core Based Tree) multicast protocol. Group key distribution forms a part of the process of the junction of a system to the group tree. The backdraw of this solution is that it is not independent from the routing protocol and cannot react in the case of dynamic group.

As for the approach GKMP [14], it is specified to work in an environment of a multi-levels of security. It allows an entity, group manager, to create and to distribute group keys by cooperating with other members of the group. The centralization of the group management is one of the defaults of this proposition. Also, the number of exchanged messages at the moment of group initialization is significant.

All these works are only attemps because the securization of IP multicast is very complicated due to problems coming from the scalability of IP multicast [17]: group size, address allocation problems, limited storage space, flow control, interaction between routing protocols intra/inter domains, states to be memorized by routers, and signalization between routers.

6. Conclusion

In this article, we have presented a general survey on the state of the art of the group communication security. We have noted that the problematic of the security of this type of communication appears, for dynamic and expanded group, in two forms of scalability problem : **1 affect n** and **1 does not equal n**.

We have focused our study on the approaches of the multicast key establishement and the multicast security management. Also, we have presented and compared different approaches of multicast key establishment. We have showed that the hierarchical approches resolve the failure **1 does not equal n**.

Also, we have presented approaches of group access control. The works presented by [16, 11, 12] divide the group into sub-groups and therefore resolve the failure **1 affect n**, but they are less efficient than [14, 19, 20] for the transmission of group communications.

Finally, we conclude that there is, presently, no satisfying solution for the multicast security. A such solution should provide [8]: minimal time of group configuration, traffic as reduced as possible, dynamic group, independancy of routing protocols, confidentiality, integrity, and authentication of data, decentralization of group management.

Having these aims, we have specified a new group key distribution protocol [9]. At present, we are using NS (Network Simulator) to validate it.

References

[1] R. Atkinson and S. Kent. Security Architecture for the Internet Protocol, November 1998. Request For Comments rfc-2401.

[2] D. Balenson, D. McGrew, and A. Sherman. Key Management for Large Dynamic Groups : One-way Function Trees and Amortized Initialization, February 1999. Internet draft.

[3] T. Ballardie. Scalable Multicast Key Distribution, may 1996. Request For Comments rfc-1949.

[4] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-Secure Key Distribution for Dynamic Conferences. Advances in Cryptology : proceedings of Crypto92, E. F. Brickell, Ed., LNCS 740, Springer-Verlag (1992), 471-486, 1992.

[5] M. Burmester and Y. G. Desmedt. Effi cient and Secure Conference-Key Distribution. Secure Protocol, M. Lomas, Ed. , LNCS 1189, Springer-Verlag, 119-130, 1997.

[6] R. Canetti, P. Cheng, D. Pendarakis, J. Rao, R. Rohatgi, and D. Saha. An Architecture for Secure Internet Multicast, February 1999. Internet draft.

[7] R. Canetti and B. Pinkas. A Taxonomy of multicast security issues, May 1998. Internet draft.

[8] G. Chaddoud. La sécurité dans IPv6 pour des applications multipoints. Stage de dea, LORIA, july 98.

[9] G. Chaddoud, I. Chrisment, and A. Schaff. Baal : Secure and Dynamic Group Communications, Mars 2000. Submitted to CFIP2000, in french.

[10] A. Fiat and M. Noar. Broadcast Encryption. Technical report, 1993.

[11] T. Hardjono, B. Cain, and N. Doraswamy. A Framework for Group Key Management for Multicast Security, August 1999. Internet draft.

[12] T. Hardjono, B. Cain, and I. Monga. Intra-Domain Group Key Management Protocol, August 1999. Internet draft.

[13] D. Harkins and D. Carrel. The Internet Key Exchange (IKE), November 1998. Request For Comments rfc-2409.

[14] H. Harney and C. Muckenhirn. Group Key Management Protocol (GKMP) Architecture, July 1997. Request For Comments rfc-2094.

[15] D. Maughan, M. Schertler, M. Schneider, and J. Tumer. Internet Security Association and Key Management Protocol (ISAKMP), November 1998. Request For Comments rfc-2408.

[16] S. Mittra. Iolus: A Framework for Scalable Secure Multicasting. ACM-SIGCOMM'97, septembre 1997.

[17] J. Pansiot and A. Alloui. Routage multipoint interdomaine, september 1999. Ecole d'été RHDM'99.

[18] M. Steiner, G. Tsudik, and M. Wainder. Diffi e-Hellman Key Distribution Extended to Group Communication. 3rd ACM conference on Computer and Communication Security, New Delhi, India, 14-16March 1996.

[19] D. Wallner, E. Harder, and R. Agee. Key Management for Multicast: Issues and Architecture, September 1998. Internet draft.

[20] C. Wong, M. Gouda, and S. Lam. Secure Group Communications Using Key Graphs. ACM-SIGCOMM'98, septembre 1998.